How to keep your
Trade Secrets "SECRET"

Table of Contents

- What are Trade Secrets?
- Does my Business have Trade Secrets?
- How do I protect Trade Secrets?
- Trade Secrets in IP Strategy
- Conclusion

What are Trade Secrets?

Trade secrets, also known as confidential information, consist of information that provides a business its competitive edge and is not known to the general public. A well known example of a trade secret is the formula for Coca-Cola. There is no requirement for registration and no formalities are required before such information can be protected as a trade secret. As long as the information remains a secret, there is protection against disclosure.

Confidentiality of the information is said to have been breached upon a disclosure while under an obligation to maintain confidentiality. Legal action can be taken for a breach of confidence. To determine if there is a breach of confidence, the Court will consider whether:

- The information was confidential (secret) to the company;
- The information was let out in breach of a promise of confidence or secrecy;
- The information was used or is about to be used without the owner's consent resulting in detriment to the owner.

Upon disclosure, the damage done may be permanent. Depending on the extent of the disclosure, there may be little you can do to "undo" the disclosure apart from restraining against further unauthorized disclosures and suing for damages. It is thus important to note that prevention is key to trade secret protection, i.e. controlling access to the trade secret. In the current state of technological advancement where information can be easily copied, transferred across media and shared in blogs and social networks, a holistic approach to the information and security infrastructure becomes important especially if your trade secret is also kept in digital formats (eg, information stored in IT databases).

Does my Business have Trade Secrets?

Yes, your business will definitely have trade secrets. Trade secrets can be customer databases, supplier lists, price lists, methods of manufacture, proprietary business processes, recipes, R&D journals, product prototypes and pre-launch product design & marketing information. There is no

limitation to the subject matter. It generally involves information that has commercial value and is known to a restricted group. When disclosed to unauthorized parties, your business stands to lose its competitive advantage. For example, your restaurant is reputed for a special dish prepared according to a secret recipe. This recipe has been passed down for generations and no other restaurants are able to prepare the dish as well as you could. Imagine the loss to your business if the recipe is leaked to outsiders when the whole restaurant business is dependent on keeping the recipe secret for its survival? In another instance, imagine what will happen to your business if your competitor gets hold of your customer database?

Trade secret protection is useful if you want to keep the information secret indefinitely. It is advisable to conduct regular trade secret audits to identify and prioritize your business' trade secrets based on their value. Once they have been identified, the next crucial step is to ensure the information can be shown to be and continue to be confidential where access is granted on a need-to-know basis. It is important to keep an audit trial of the access to the confidential information, whether it is physical or digital. It will make useful evidence in the event of a breach.

Trade secret protection may not apply in every situation. For example, where it is possible through a process of reverse engineering to derive the same information as that contained in the trade secret, trade secret protection would not be suitable. In such cases, patent protection may be a more appropriate form of protection. Of course, it will then be necessary for a business to consider whether patent protection is feasible. Businesses should bear in mind the cost involved and also take into account the life cycle of the product balanced against the time required to obtain a patent and the maximum period of patent protection available. In general protection is limited to 20 years from the date the patent is applied for.

How do I protect Trade Secrets?

For managing disclosures to employees, you may consider the following:

Employment Contract	Clauses to consider including in employment contracts: • Confidential information is properly defined in the employment contract; • Contract contains confidentiality clauses which will survive termination when employee leaves your employment; • Clauses that provide for consequences in the event of a disclosure, eg damages, injunctive relief to prevent the continuance of the disclosure, and delivery up of documentation containing the confidential information.

	Employers may sometimes impose a limited trade restraint on its key employees. This may be practised in industries where the competition for human resource among the players is keen and the industry requires specialized skills. This is a clause in the employment contract that restricts the employee from joining a competitor after leaving your employment. Such a restriction may be stipulated by way of time or geographical boundary. It is important to note that these confidentiality and trade restraint clauses must be carefully worded. Under the law, a restraint of trade is contrary to public policy and is unenforceable unless it is reasonable. For example, forbidding an employee from seeking employment in a similar industry for a long period like 10 years and anywhere in the world is likely to be regarded as unreasonable as it restricts the employee's ability to earn a living. Restraining clauses are however enforceable if they serve to protect a legitimate interest and the restraint is reasonable, i.e. it sufficiently protects the employer's interest and nothing more.
Employee Education	Measures to educate and remind employees of the meaning of confidentiality and the appropriate steps to be taken to safeguard confidential information. For example: • confidential documents should be labeled "confidential" and access should be restricted appropriately; • confidential matters should not be discussed in public, along corridors or in any online forum; • disclosure should be on a need-to-know basis; • employees should be i) reminded not to share their login id and password with colleagues as it may lead to unauthorized access; ii) reminded not to write their password on paper; iii) educated on how to come up with creative yet easy-to-remember passwords that will pose a challenge for potential intruders.
IT Security Infrastructure	The IT infrastructure should be designed to prevent unauthorized access to restricted information. Some IT measures include: • restricting access via login id, password and firewalls; • implementing 2 factor authentication to further control access for sensitive

	information; • encrypting data or emails when stored, before and during transmission via a network or internet, depending on the sensitivity of the information. Regular security audit by independent auditors may be considered. While security is important, the IT implementation must of course take into account the cost involved as well as the ease-of-use aspect so as not to hamper users' productivity. The precise measures to be implemented is ultimately a commercial decision balancing the value of the confidential information against the cost and administrative inconvenience.
Data Protection Policy	A company's policy on data protection should be drawn up and measures to safeguard confidential data should be implemented. This is especially so for sensitive financial information and customers' data. For example, a company which holds customers' personal data should have the necessary safeguards to prevent unauthorized access by employees or external parties such as its IT support vendors or consultants. Access to such information should be granted on a need-to-know basis. Regular review of the data protection policy may be considered.
Exit Interview	Employees leaving the company should be reminded of their continuing responsibility to maintain confidentiality and to return any information or document which contains confidential information.

For disclosures to external parties, you may consider the following:

External Contractors	When you engage the services of external contractors, include confidentiality clauses in the service agreement. This will obligate the contracting company and his employees to maintain confidentiality of the information that they come into contact with in the course of providing the service to you. These external parties may be vendors, consultants, interns or temporary staff. It is important to restrict access by external IT personnel providing support to the IT

	infrastructure, who are non-employees, to the confidential information stored in the relevant systems only.
Information Disclosure	If, for a specific reason, you wish to disclose confidential information to an external party, you should insist that the party who will receive the information sign a non-disclosure agreement (NDA). It is only after signing the NDA that you should disclose the confidential information. In particular, if you are considering filing applications for patents or registered designs, you must be aware that novelty is one of the requirements for registration. Once disclosed to any external party, in the absence of confidentiality obligations on the part of the external party, novelty is destroyed. Verbal NDAs are valid agreements but it is extremely difficult to prove the existence of such agreements in Court.

Trade Secrets in IP Strategy

In many products we use today, it is easy to spot a multi-pronged IP strategy applied to a single product. An IP strategy usually consists of a portfolio of registrable IP rights like patents, trade marks and designs, and non-registratable IP rights like copyright and trade secrets.

Patents and trade secrets are opposites in the aspect of disclosure. The publication step in a patent process involves the specification of the invention becoming part of the prior art and the specification would then no longer be eligible for trade secret protection. To determine whether a patent or trade secret is more suitable as a form of protection, questions you might ask are, how easy it is to reverse engineer the product/process; what is the possible commercial lifespan of the invention and what is the value of the invention. This does not however mean you cannot use trade secrets once the patent route is chosen. Trade secrets are not limited to inventions. Other information that has commercial value and is known to a restricted group may qualify for trade secret protection. Often, it is necessary to have access to the confidential information surrounding a patent to effectively exploit the patent.

Using a mobile phone as an example to illustrate the multiple forms of IP, there could possibly be protection for its circuitry layout design, copyright for its ringtones and user manual, trade mark for its brand, design protection for its appearance, and patents for many of its electronic and telecommunication parts and features. Trade secrets may be applied to the chemical composition of the material used for the mobile phone cover or a specific manufacturing process that is not patented.

An overall IP strategy should provide the necessary protection and should be able to withstand fierce market conditions. To ascertain whether your IP strategy is effective, you should seek the advice of an IP lawyer or expert before implementing it.

Conclusion

Look no further. There may be many undiscovered gems in your business – information your competitors would be most keen to know about your business. The good news is trade secret protection does not require any formalities or fee, only the cost of safeguarding them against inappropriate disclosures via oral, written or digital communication measures, intentionally or otherwise.

Useful Resources

1. IPOS has an IP Management programme catered for SMEs. Please click here for more info or contact IPOS at Tel 6339 8616.
2. For a list of IP professionals, please refer to SNIPS here.
3. For other topics featured on IP management, please refer to IP Knowledge Kaleidoscope here.

Acknowledgement

We would like to thank Mr Lau Kok Keng, Partner, Rajah & Tann LLP for his valuable feedback.

Feedback

We seek your views on how IP Knowledge Kaleidoscope can serve the business community better. Please email us your feedback to ipos_enquiry@ipos.gov.sg.

Information as of 29 Sep 2010
© 2010 Intellectual Property Office of Singapore

Disclaimer: This article is for general information only and is not intended to be a substitute for professional advice. Please seek independent legal, business or other relevant specialist advice, where necessary, and not merely rely or act on any information provided here.

Intellectual Property Office of Singapore

51 Bras Basah Road #04-01, Plaza By The Park, Singapore 189554
Tel: (65) 63398616 Fax: (65) 63390252 http://www.ipos.gov.sg/

IPOS
INTELLECTUAL PROPERTY OFFICE OF SINGAPORE